UAV 와 GCS 간 Wi-Fi 통신 보안 향상 기법

윤지영, 이효준, 박경준
대구경북과학기술원

{hailey_yoon; hj.lee; kjp} @dgist.ac.kr

Security Enhancement in Wi-Fi Communication Between UAV and GCS

Jiyoung Yoon, Hyojun Lee, Kyung-Joon Park
Daegu Gyeongbuk Institute of Science & Technology (DGIST)

요 약

최근 활용 범위가 넓어지는 드론이라 불리는 UAV(Unmanned Aerial Vehicle)는 점차 성장하여 2026 년 세계 드론 시장은 약 820 억 달러에 이를 것으로 예상된다. UAV 는 RC transmitter, Bluetooth, Wi-Fi 등의 무선 통신으로 GCS(Ground Control Station)와 연결되어 미션을 받고 수행한다. 본 논문에서는 현재 PX4, Ardupilot 에서 제안하는 Wi-Fi telemetry module 에서 동작하는 firmware 의 프로세스와 해당 프로세스의 문제점에 대해 서술하고 이 문제점을 해결할 수 있는 UAV 와 GCS 간 Wi-Fi 통신의 보안 향상 기법을 제안한다.

Ⅰ. 서 론

드론이라 불리는 무인항공기(UAV: Unmanned Aerial Vehicle)는 레저, 미디어 및 엔터테인먼트 군사 등의 목적과 함께 건설, 광업 산업, 생명 구조 활동 등 활용 범위가 점차 넓어지고 있다. 국토부에 따르면 세계 드론 시장은 연 29%씩 성장하여 2026 년 약 820 억 달러에 이를 것으로 예상한다. 드론은 4 차 산업혁명의 테마인 CPS(Cyber Physical Systems)의 중요한 애플리케이션 중 하나로 대두되고 있다 [1, 2].

UAV 는 RC transmitter, Bluetooth, Wi-Fi 등 다양한 매체를 이용하여 제어할 수 있으며, UAV 는 해당 매체를 통해 GCS(Ground Control Station)와 연결되어 비행한다. 이렇게 연결된 GCS 는 UAV 에게 비행 임무와 관련된 명령을 내리고 이에 대한 UAV 의 비행 상태 및 여러 센서들의 상태 정보를 모니터링할 수 있다.

본 논문에서는 UAV 와 GCS 간 Wi-Fi 통신에서의 보안을 강화하기 위해 기존의 여러 시스템에서 제안하고 있는 MavESP8266 펌웨어의 문제점을 찾고 이에 대한 해결방안을 제시한다. MavESP8266 펌웨어는 UAV 가 MAVLink 프로토콜을 이용하기 위해 UAV 에 장착된 Wi-Fi 모듈에 설치하는 펌웨어이다. MAVLink 프로토콜은 UAV 와 GCS, 그리고 UAV 에 탑재된 여러 구성 요소들 사이에서 통신하기 위한 프로토콜이며 DJI, Parrot 사의 제품뿐만 아니라 많은 UAV 에서 사용하는 대표적인 프로토콜이다.

Ⅱ. 본론

GCS 와 UAV 가 무선 통신으로 연결되어 있을 때 악의적인 공격자가 UAV 의 상태 정보, 미션 정보를 도청할 수 있다. 그러나 공격자가 GCS 인척 UAV 에게 명령을 보내는 스푸핑, 패킷 인젝션 공격은 인명, 재산적 피해를 초래할 수 있는 심각한 위험 요소이다. 그래서 이를 방지하기 위한 노력이 필요하다. 그러나 우리는 UAV 가 MavESP8266 펌웨어를 이용한 Wi-Fi 통신을 할 경우 이 같은 위험에 더 쉽게 노출되어 있다는 것을 확인했다.

본 논문에서는 UAS(Unmanned Aerial System)를 구성하기 위해 하드웨어는 Pixhawk2, firmware 는 ArduCopter V3.6.8 Hexa 를 사용하였다. 그리고 Wi-Fi 네트워크 환경을 구성하기 위해 Pixhawk2 의 telemetry1 포트에 ESP8266 모듈을 연결하였다. Wi-Fi 모듈인 ESP8266 의 펌웨어로 MavESP8266 을 사용한다. 이는 PX4, Ardupilot 측에서 제안하는 모델로 Pixhawk 를 이용한 UAV 일 경우 많이 쓰이는 모델이다. ESP8266 모듈은 AP 의 역할을 하며 GCS 에서 Wi-Fi 네트워크에 접속 후 UDP 로 UAV 와 연결을 맺는다.

UAV 와 GCS 가 연결되는 과정은 다음과 같다. GCS 에서 UAV 의 네트워크에 접속을 한 뒤 MAVLink message 가 담긴 UDP 를 통해 UAV 와 연결을 한다. 연결 초기에 GCS 에서 UAV 에게 parameter 를 요청하면 UAV 는 자신의 parameter 를 전송한다. 그리고 주기적으로 서로 Heartbeat message 를

```
1 :  if UDP packet received
2 :      parse UDP packet to MAVLink message
3 :      if GCS is not connected yet
4 :          _IP ← source IP of UDP packet
5 :      Heartbeat check
6 :      CRC check
7 :      send MAVLink message to Pixhawk
```

<그림 1> 기존 MavESP8266 패킷 처리 알고리즘.

송신하며 UAV 는 GCS 에게 자신의 상태, 미션 등의 정보를 주기적으로 송신한다. 이러한 연결 과정에서 UAV 인 Pixhawk 의 firmware 인 ArduCopter V3.6.8 Hexa 는 GCS 가 원하는 정보만 전송할 뿐 아무런 개입이 없으며 GCS 에 대한 네트워크 정보가 없다. 이는 MavESP8266 에서 관리된다.

MavESP8266 을 플래싱한 UAV 의 Wi-Fi 모듈의 경우, UDP 패킷을 받으면 그림 1 과 같은 프로세스를 통해 동작한다. UAV 가 GCS 와 아직 연결되지 않았다면 처음 받은 UDP 패킷의 IP 를 Wi-Fi 모듈에서 GCS 의 IP 로 저장한다. 그러나 UAV 는 이 프로세스를 거치고 나면 GCS 와 연결되었다고 판단 후, UDP 패킷의 *Source_IP* 를 검사하지 않고 패킷을 받아들인다. 그림 1 은 이 프로세스를 간단하게 나타낸 그림이다.

이 같은 프로세스는 다음과 같은 문제점이 있다. GCS 와 연결된 후에는 악의적인 공격자가 Wi-Fi 에 접근할 수만 있다면 GCS 인척 UDP 패킷의 *Source_IP* 를 바꿀 필요 없이 MAVLink message 를 주입시키는 행동만으로 UAV 를 쉽게 공격할 수 있다는 점이다. 이와 같은 Wi-Fi 는 대부분 Wi-Fi 비밀번호를 초기 설정 그대로 유지하는 경우가 있어 공격이 매우 쉬울 수 있다.

그림 2 는 실제 실험에서 패킷을 캡처한 그림이다. 우리는 실제로 GCS 와 UAV 를 연결하여 비행을 하는 실험을 하였다. 공격자는 Wi-Fi 통신에 들어온 후, UAV 에게 모터의 동작을 즉각적으로 종료시키는 명령인 *disarm_command* 패킷을 주입시킴으로써 UAV 를 바로 추락시킬 수 있었다. 그림 2 는 IP 가 192.168.4.1 인 UAV 와 IP 가 192.168.4.2 인 GCS 와의 통신을 보여준다. 빨간 상자가 공격 시점인데, 이를 중심으로 공격 전의 상황에서 GCS 가 명령을 보내지 않았음에도 불구하고 빨간 상자에서 UAV 가 GCS 에게 명령에 대한 대답인 *COMMAND_ACK* 메시지를 보내는 것을 확인할 수 있다. 이는 다른 *Source_IP* 를 가짐에도 불구하고 이를 GCS 로 받아들인 후 GCS 에게 ACK 를 보내는 것을 나타낸다.

이 같은 문제점을 해결하기 위해 MavESP8266 에서 UDP 패킷을 받고 처리하는 프로세스를 수정할 필요가 있었다. 문제점은 UAV 가 GCS 와 연결된 후 UDP 패킷을 받을 때 신원을 확인하지 않는 점이기 때문에 우리는 그림 3 과 같이 GCS 와 연결된 후 UDP 패킷을 받을 때 신원을 확인하는 프로세스를 추가해 주었다. 수정된 MavESP8266 을 다시 Wi-Fi 모듈에 플래싱 시켜준 후 이전과 같은 실험을 하였을 때 UAV 가 추락하지 않는 것을 확인할 수 있었다.

No.	Source	Destination	Protocol	Length	Info
4030	192.168.4.1	192.168.4.2	MAVLink 1.0	158	ATTITUDE AHRS2 AHRS3
4031	192.168.4.1	192.168.4.2	MAVLink 1.0	70	VFR_HUD
4032	192.168.4.1	192.168.4.2	MAVLink 1.0	151	SERVO_OUTPUT_RAW RC_CHAN
4033	192.168.4.1	192.168.4.2	MAVLink 1.0	189	SYS_STATUS POWER_STATUS
4034	192.168.4.1	192.168.4.2	MAVLink 1.0	101	POSITION_TARGET_GLOBAL_INT
4035	192.168.4.1	192.168.4.2	MAVLink 1.0	178	STATUSTEXT MISSION_ITEM_
4036	192.168.4.1	192.168.4.2	MAVLink 1.0	72	TERRAIN_REPORT
4037	192.168.4.1	192.168.4.2	MAVLink 1.0	156	BATTERY_STATUS EKF_STATU
4038	192.168.4.1	192.168.4.2	MAVLink 1.0	158	ATTITUDE AHRS2 AHRS3
4039	192.168.4.1	192.168.4.2	MAVLink 1.0	70	VFR_HUD
4040	192.168.4.1	192.168.4.2	MAVLink 1.0	180	RAW_IMU SCALED_IMU2 SC
4041	192.168.4.1	192.168.4.2	MAVLink 1.0	59	HEARTBEAT
4042	192.168.4.1	192.168.4.2	MAVLink 1.0	86	PARAM_VALUE COMMAND_ACK
4043	192.168.4.1	192.168.4.2	MAVLink 1.0	114	GLOBAL_POSITION_INT LOCA
4044	192.168.4.1	192.168.4.2	MAVLink 1.0	158	ATTITUDE AHRS2 AHRS3
4045	192.168.4.1	192.168.4.2	MAVLink 1.0	70	VFR_HUD
4056	192.168.4.1	192.168.4.2	MAVLink 1.0	151	SERVO_OUTPUT_RAW RC_CHAN
4057	192.168.4.1	192.168.4.2	MAVLink 1.0	189	SYS_STATUS POWER_STATUS

<그림 2> 실험을 통한 UAV 와 GCS 간 패킷 교환.

```
1 :  if UDP packet received
2 :      parse UDP packet to MAVLink message
3 :      if GCS is not connected yet
4 :          _IP ← source IP of UDP packet
5 :      else
6 :          if _IP ! = source IP of UDP packet
7 :              exit the process
8 :      Heartbeat check
9 :      CRC check
10 :     send MAVLink message to Pixhawk
```

<그림 3>수정된 MavESP8266 패킷 처리 알고리즘.

Ⅲ. 결론

본 논문에서는 다양한 네트워크 공격에 노출되어 있던 기존의 UAV 에 탑재되는 MavESP8266 의 문제점을 찾고 UAV 와 GCS 간 Wi-Fi 통신에서의 보안을 강화하기 위해 이에 대한 해결방안을 제시하였다. 이는 UDP 패킷을 받은 후 신원을 확인하는 프로세스를 추가함으로써 문제점을 해결할 수 있었다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부에서 지원하는 DGIST 기관고유사업에 의해 수행되었습니다(19-ST-02).

참 고 문 헌

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," Computer Communications, vol. 36, issue 1, pp. 1-7, December 2012.

[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2204-2215, November 2014.